Fraunhofer
IIS

easyDCP KDM Generator
easyDCP KDM Generator+

User manual

Version
1.4

Date
Erlangen, 04/05/2015

Contents

1	**Welcome**	**3**
2	**Feature Overview**	**4**
3	**Installation**	**5**
3.1	Installation on Windows	5
3.2	Uninstallation on Windows	7
3.3	Demo Mode Restrictions	9
3.4	License Activation and Certification	9
3.5	Software Upgrade	9
4	**Generating KDMs**	**10**
4.1	The graphical user interface	10
4.1.1	General Settings tab	11
4.1.2	Advanced Settings	13
4.1.3	Output tab	14
4.1.4	Options menu	15
5	**KDM Signature**	**16**
6	**Distribution KDM**	**18**
6.1	Application Data and Settings	20
7	**Using the command line program**	**21**
7.1	Parameters	21
7.2	Date and Time Specification	22
8	**Creating proper Digest Files**	**23**
9	**Frequently Asked Questions (FAQs)**	**24**
10	**Contact**	**26**

1 Welcome

Thank you for purchasing easyDCP KDM Generator or easyDCP KDM Generator+ software.

easyDCP KDM Generator allows you to generate KDMs of your encrypted DCP in a fast and convenient manner. Based on an easyDCP Digest file, which is created by easyDCP Creator+ along with each encrypted DCP, it is possible to generate KDMs or Distribution KDMs for digital cinema servers or mastering stations.

easyDCP KDM Generator+ also manages its own private and public key-pair, therefore enabling you to receive Distribution KDMs. A Distribution KDM is technically identical to a regular KDM. The difference is that it's recipient is another mastering station or KDM creation tool in the post-production or distribution chain. This feature makes easyDCP KDM Generator+ usable independently from easyDCP Creator+ and enables you to handle large KDM creation and distribution jobs for encrypted DCPs created by any mastering station.

easyDCP KDM Generator(+) is able to generate KDMs in SMPTE or InterOp conformity mode. By default, the proper mode is selected automatically based on the recipient's certificate's conformity. easyDCP KDM Generator(+) is laid out to batch process large KDM creation jobs. In addition to targeting a single server certificate you can also specify a directory containing as many as hundreds of server certificates. easyDCP KDM Generator(+) will generate KDMs for all detected valid server certificates within seconds. Thanks to a configurable digital signature, you can make sure to deliver trustable keys to your customers. easyDCP KDM Generator(+) requires no special hardware.

2 Feature Overview

	easyDCP KDM Generator	easyDCP KDM Generator+
Creates valid KDMs	x	x
Graphical User Interface	x	x
Usable from command-line (CLI)	x	x
Creates SMPTE or InterOp KDMs	x	x
Reads proprietary easyDCP Digest File	x	x
Reads Distribution KDM (DKDM)		x
Independent of easyDCP Creator+		x
Available for Windows 7	x	x
Available for Mac (10.6 or newer)	x	x

3 Installation

The installation of the easyDCP KDM Generator(+) will only take a few minutes. You can download one single executable setup file (for Windows) or one single package file (for Mac) at the following address:

http://www.easydcp.com/

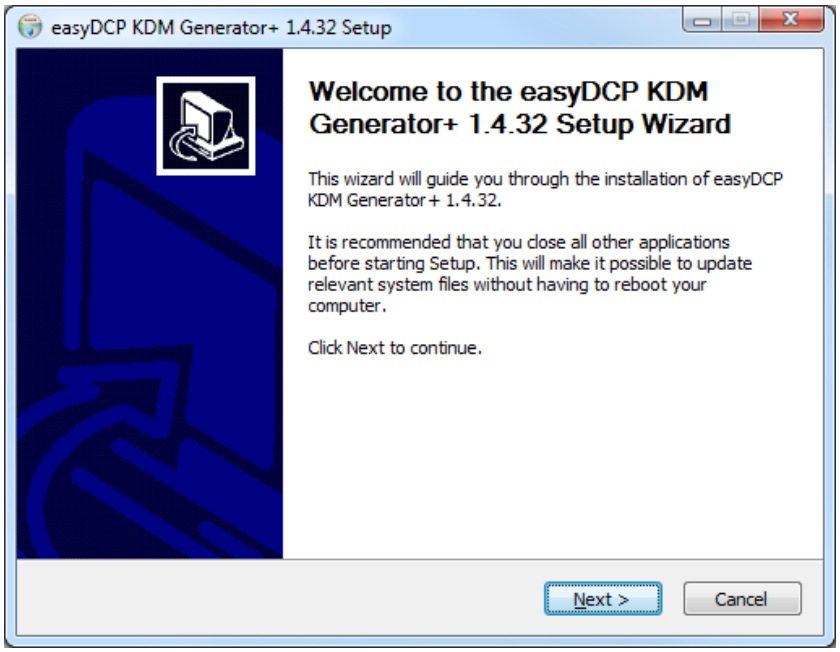
Please check regularly to make sure you have the latest version.

To install easyDCP KDM Generator(+), make sure you have the required rights (i. e. admin rights).

3.1 Installation on Windows

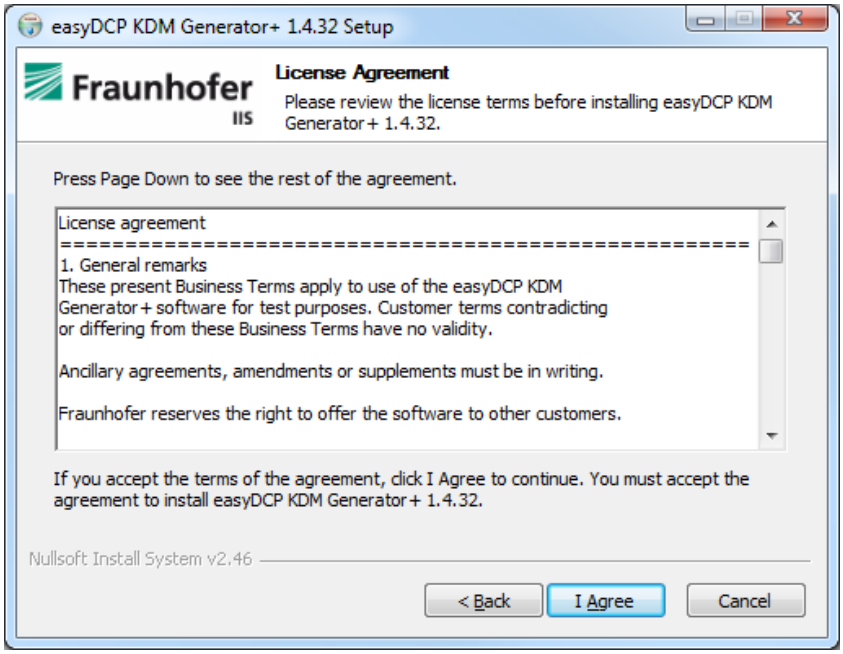
Under windows systems double click on the one executable setup file you received from us or downloaded at the easyDCP Homepage.

The setup start window should appear:


easyDCP KDM Generator+ 1.4.32 Setup
Welcome to the easyDCP KDM Generator+ 1.4.32 Setup Wizard
This wizard will guide you through the installation of easyDCP KDM Generator+ 1.4.32.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel

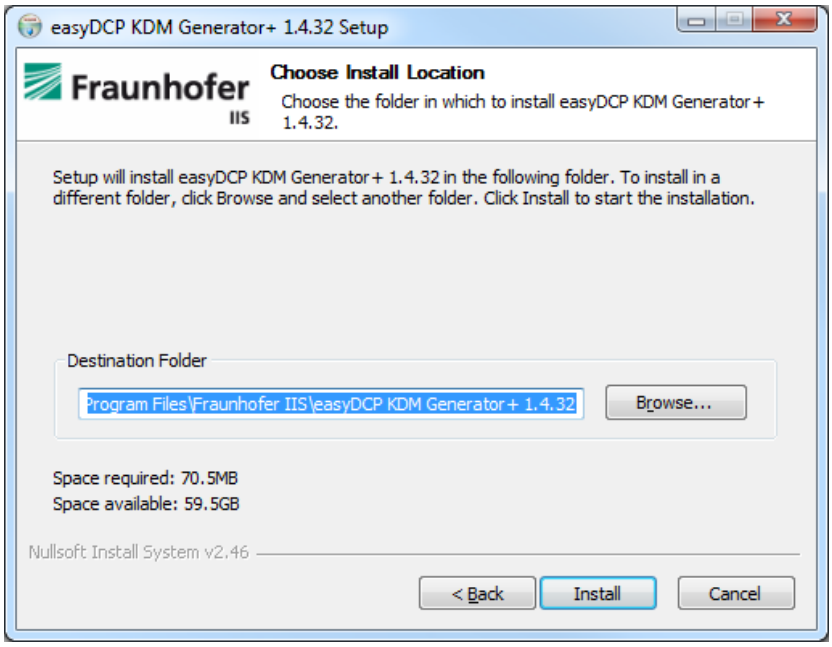
Press „`Next >`“ to continue installation or „`Cancel`“ to abort.

After pressing „Next >“ the License Agreement window appears:


easyDCP KDM Generator+ 1.4.32 Setup
Fraunhofer IIS
License Agreement
Please review the license terms before installing easyDCP KDM Generator+ 1.4.32.
Press Page Down to see the rest of the agreement.
License agreement
1. General remarks
These present Business Terms apply to use of the easyDCP KDM Generator+ software for test purposes. Customer terms contradicting or differing from these Business Terms have no validity.
Ancillary agreements, amendments or supplements must be in writing.
Fraunhofer reserves the right to offer the software to other customers.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install easyDCP KDM Generator+ 1.4.32.
Nullsoft Install System v2.46
< Back
I Agree
Cancel

Please read the license agreement carefully. To scroll through the text use the slide bar on the right side. This window may differ from yours regarding which version of easyDCP KDM Generator you are installing.

After pressing “I Agree” the installation location setup dialog appears:

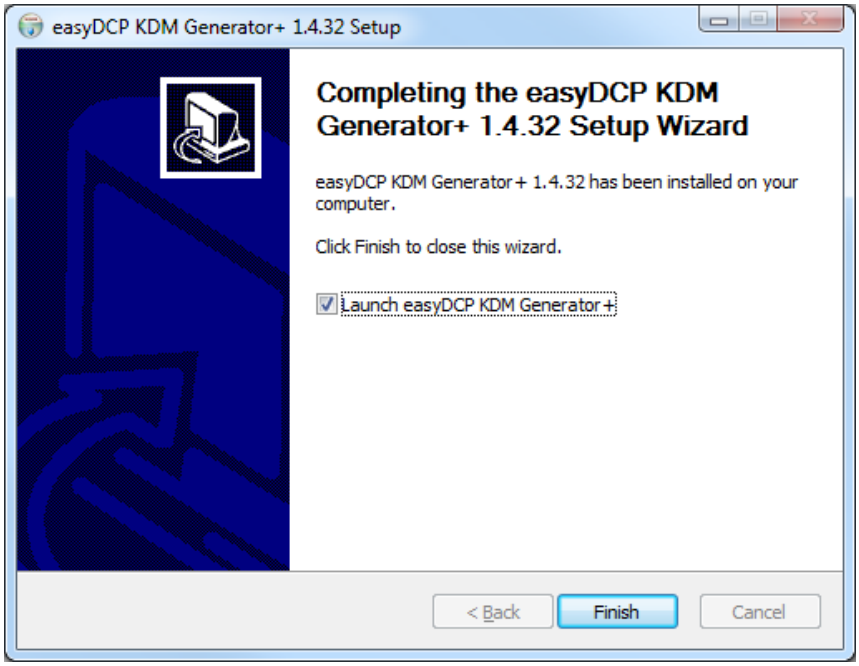

easyDCP KDM Generator+ 1.4.32 Setup
Fraunhofer IIS
Choose Install Location
Choose the folder in which to install easyDCP KDM Generator+ 1.4.32.
Setup will install easyDCP KDM Generator+ 1.4.32 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
Program Files\Fraunhofer IIS\easyDCP KDM Generator+ 1.4.32
Browse...
Space required: 70.5MB
Space available: 59.5GB
Nullsoft Install System v2.46
< Back
Install
Cancel

Setup will install easyDCP KDM Generator(+) in the “Destination Folder”. To install in a different folder, type the folder of your choice into the

text field or click the "Browse" button to select a folder. Make sure you have the certain rights (i. e. admin rights) to write to that folder.

During installation some entries will be made to the windows registry of your operating system (e.g. for association of the file type extension for easyDCP Digest files *.dcpdig, uninstalling information, licensing information). These registry entries will be removed during uninstall (see 3.2).

After finishing the installation process, the following dialog appears:


easyDCP KDM Generator+ 1.4.32 Setup
Completing the easyDCP KDM Generator+ 1.4.32 Setup Wizard
easyDCP KDM Generator+ 1.4.32 has been installed on your computer.
Click Finish to close this wizard.
Launch easyDCP KDM Generator+
< Back
Finish
Cancel

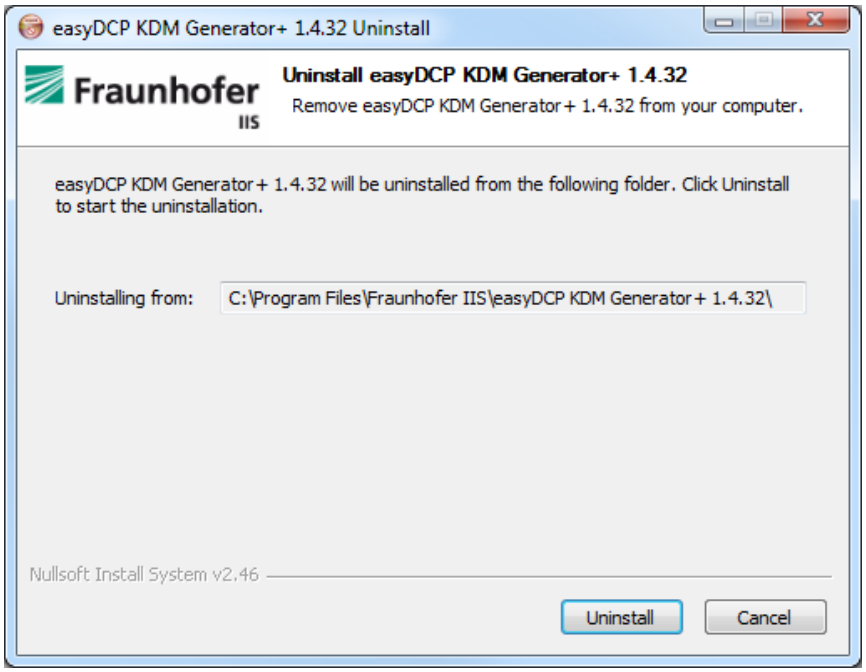
After successful installation process you can find shortcuts to easyDCP KDM Generator(+) in the Windows start menu and on the desktop.

3.2 Uninstallation on Windows

In order to uninstall all easyDCP KDM Generator(+) components (including the windows registry entries) run "Uninstall easyDCP KDM Generator" in the start menu entry. Make sure you have sufficient rights (e.g. admin rights) to do such operations.

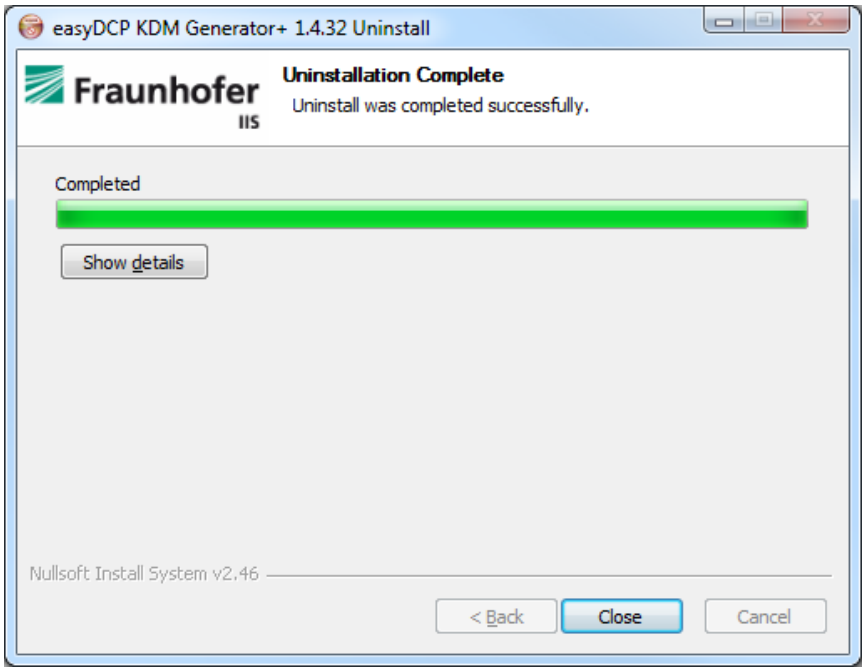
If however your easyDCP KDM Generator entry does not exist anymore in the Windows start menu, go to the folder where you installed easyDCP KDM Generator and run the executable "Uninstall easyDCP KDM Generator.exe" by double clicking.

After running the easyDCP KDM Generator Uninstaller, the following window should appear:


easyDCP KDM Generator+ 1.4.32 Uninstall
Fraunhofer IIS
Uninstall easyDCP KDM Generator+ 1.4.32
Remove easyDCP KDM Generator+ 1.4.32 from your computer.
easyDCP KDM Generator+ 1.4.32 will be uninstalled from the following folder. Click Uninstall to start the uninstallation.
Uninstalling from:
C:\Program Files\Fraunhofer IIS\easyDCP KDM Generator+ 1.4.32\
Nullsoft Install System v2.46
Uninstall
Cancel

All files and directories will be deleted, except user files (e.g. licenses, certificates). Directories that include user files will not be removed. This makes sure that, when you update easyDCP KDM Generator(+) to a newer version, your license file and certificates will be kept.

After pressing „`Uninstall`“ the following window should appear:



After a few seconds, the uninstallation of easyDCP KDM Generator(+) should be complete. There are no more files left except user files (e.g. certificates, licenses). The windows registry is cleaned up. The file type association with the extension `*.dcpdig` for easyDCP Digest files is removed.

Press the button „`Show details`“ to show details which files were deleted.

3.3 Demo Mode Restrictions

In the demo version of easyDCP KDM Generator(+) you may only create KDMs with a valid period of two days or less. Furthermore the demo version provides automatically generated signer and server example certificates only.

3.4 License Activation and Certification

By default, the commercial version of easyDCP KDM Generator(+) will start up in unlicensed mode. **In this version a valid license is necessary. Otherwise the generation of KDM(s) will not work.** To request your personal license and certificates select “Request License & Certificates” from the help menu. A dialog pops up and will ask to fill in some details. Enter the licensee’s name, the URL that shall be stated in the custom signer and server (easyDCP KDM Generator+ only) certificates and a password that is used to protect access to the certificates. If the computer is connected to the Internet, click the “submit” button. The default web-browser will open www.easydcp.com, where further instructions will guide you through the purchase process.

After the purchase, a link to the commercial installer as well as a zip file with the License and certificates will be available for download within your user account at www.easydcp.com. The zip file can be dragged & dropped into the commercial easyDCP KDM Generator installation to unlock it.

3.5 Software Upgrade

To upgrade easyDCP KDM Generator log into your user account at www.easydcp.com.

Before installing a new version, it is recommended to uninstall your existing version of easyDCP KDM Generator(+). Make sure your license is valid for the new version by reviewing the license information (hit ‘F2’). If you need a new license for the new version, you may purchase it at www.easydcp.com.

4 Generating KDMs

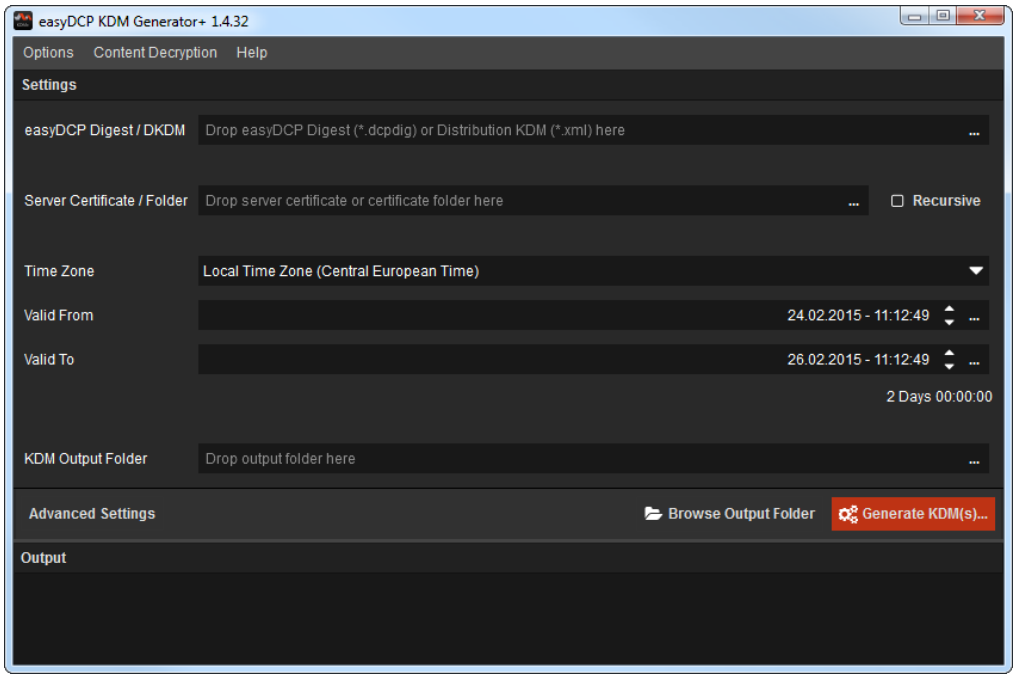
In order to generate KDMs for a Digital Cinema Package (DCPs), a key input file is required. Both easyDCP KDM Generator and easyDCP KDM Generator+ can read a proprietary easyDCP Digest file. This file is created by easyDCP Creator+ whenever an encrypted DCP is generated. The digest file describes not only the DCP's structure, but also contains all encryption keys.

Upon clicking the "`Generate KDM!`" button, easyDCP KDM Generator(+) will create KDMs for all server certificates in a single job. Using the full version of easyDCP Player+, you can test the whole procedure by issuing a KDM to your easyDCP Player+'s public server certificate. By selecting the own exported public server certificate, easyDCP KDM Generator+ can even issue a DKDM to itself. By the way, this procedure is the same when you want to issue a Distribution KDM (DKDM) for your client's mastering station.

For advanced users it is also possible to create your own digest file as described in chapter 8 (Creating proper Digest Files).

4.1 The graphical user interface

easyDCP KDM Generator(+) provides a graphical user interface which allows you to generate KDMs in a fast and convenient manner. All important settings can be applied with a few mouse clicks.



4.1.1 Settings section

The "Settings" section is the place to edit job specific input and output files or folders. You can either drag & drop files or folders onto the various input fields, or use the "…"buttons to browse for files or folders.

After all settings have been applied, the KDM batch processing job can be started by hitting the "`Generate KDM`..." button. The status messages will be printet in the output section.

A job can be aborted by hitting the same button again. An error message will appear in the output to inform the user.

"Digest / Distribution KDM"

Use this field to load the easyDCP Digest file, which contains the encrypted DCP's encryption keys. Note: A digest file contains information on all compositions of a DCP. However, a KDM only corresponds to a single composition. easyDCP KDM Generator(+) will by default create KDMs for all compositions that are listed in the digest and reference encrypted content.

The central exclusive feature of easyDCP KDM Generator+ is that it also allows to read a Distribution KDM (DKDM). The DKDM will be validated when the "Generate KDM" button is clicked. It can only be read if it was specifically issued to your easyDCP KDM Generator+ installation's public server certificate that you previously exported with the "Export public server certificate" (F7) entry in the "Content Decryption" menu and sent to the DKDM's issuer. Furthermore, the DKDMs expiration date and signature is checked.

Server Certificates Input Folder

In this field you can either point to a single public server certificate file or to a directory containing multiple public server certificate files.

By checking "Recursive" easyDCP KDM Generator(+) will include server certificates in all subfolders of a given directory also.

A public server certificate contains the server's public key which was calculated from the server's private key. The keys in a KDM will be encrypted with a single server's public key. This ensures that only the targeted server (i.e. the recipient) can decrypt the keys in the KDM, because it is the only entity that knows and has access to the private key.

It is perfectly possible to point to your own public server certificate and generate a DKDM. Subsequently you can load the DKDM into the "Digest / Distribution KDM" field. You can also issue a KDM to your easyDCP Player+ installation's public server certificate.

Usually, on the cinema server manufacturers' ftp servers you can find both the public server certificate and the signature chain that was used to sign the certificate. If you decide to trust the certificate by examining the signature certificate chain, you only need the server certificate to create a KDM. It usually has either a *.pem or *.crt suffix. easyDCP KDM Generator(+) will accept either. Furthermore, there will be pairs of certificate and chain that state "mpeg", "sha1" and "sha256". Like with DCPs, there are SMPTE and InterOp KDMs. Almost all modern servers prefer SMPTE KDMs. It is recommended to distribute only SMPTE KDMs, which are only valid if the the "sha256" server certificate version was used.

Time Zone

By default, the time zone is set to the time zone configured in the operating system. The *valid from-* and *valid to-* times are interpreted as local times of the selected time zone. During the KDM generation process these times are convertet to the equivalent UTC times. For direct use of UTC time select UTC from Time Zone.

Valid From Time / Valid To Time

By default, the validity period will be initialized to two days. By clicking on the "…" button, a calendar dialog will open.

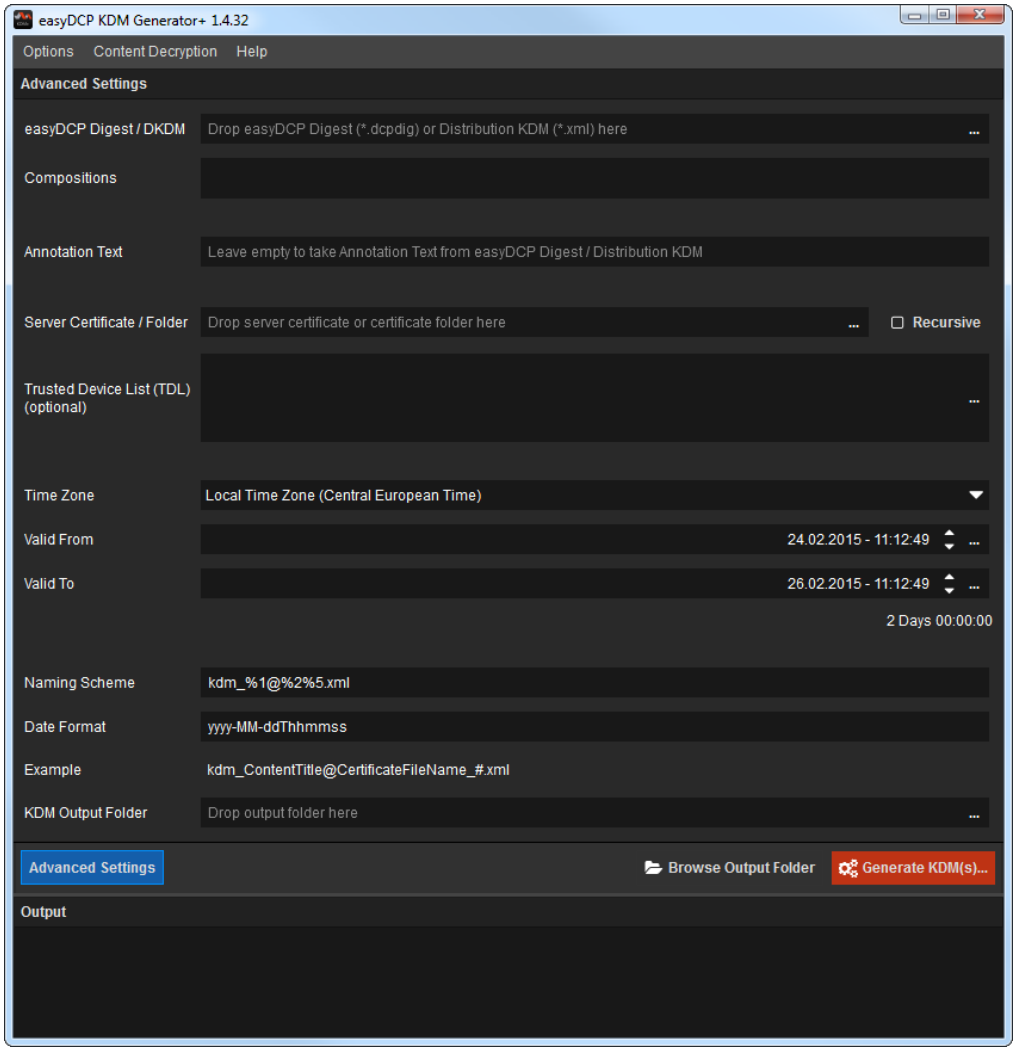
The KDM will only be valid between these two dates. Outside of this period it will not be possible to play back the corresponding encrypted DCP in a cinema. The entered dates and times are interpreted as local times according to the selected time zone.

KDM Output Folder

Specifies the directory where generated KDMs will be stored. By default, KDMs will be named
"kdm_<content_title>@<server_cert_filename>_<counter>.kdm.xml".

4.1.2 Advanced Settings

easyDCP KDM Generator offers a set of advanced options. To show or hide the advanced options click on “Advanced Settings” button.



Compositions

A list of all available compositions in the digest or DKDM. Only for selected compositions a KDM will be generated. By default all compositions are selected.

KDM Annotation Text

A KDM contains an annotation field that may contain useful information. By default the source composition's annotation text is used.

Trusted Device List

A Trusted Device List (TDL) defines peripheral equipment (like projectors, sound systems, …) which are connected to the digital cinema server. Those devices may also have certificates for themselves in order to protect the DCP content (footage). To ensure playback add certificates of trusted devices to this list.

Naming Scheme

Naming scheme for the generated KDM(s), Valid place holders are:
%1 Composition Content Title
%2 File name of server certificate
%3 UUID of the KDM
%4 Date and/or Time (see Date Formate below)
%5 Counter if KDM already exsists

Date Format

Date format used for the date place holder %4 in the naming scheme.

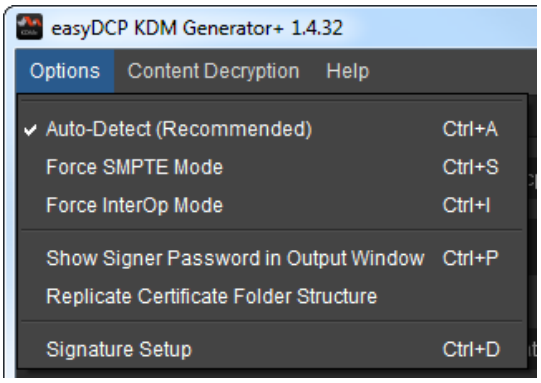
4.1.3 Output section

The output section shows a detailed description of the KDM creation process. It informs the user if all KDMs are generated successfully or if an error occurred and why. Furthermore it lists relevant properties of all server certificates.

To save the result of your process in a text file it is possible to select the content of the output window and copy & paste it to an editor. Otherwise it is not possible to edit the content of the output window.

4.1.4 Options menu

The option menu allows the user to set some additional options of the generated KDMs.



KDM conformity

By default the conformity (i.e. SMPTE vs InterOp) is automatically detected. Under normal circumstances this setting should not have to be changed. If a targeted public server certificate employs the sha256 algorithm, the KDM will be generated in SMPTE mode, otherwise in InterOp mode.

This automatic selection can be overridden by either selecting "Force SMPTE mode" or "Force InterOp mode". Note: The example signer certificates and any customized certificates obtained from Fraunhofer IIS are sha256 certificates. Therefore even an InterOp KDM will be signed with SMPTE-compliant sha256 signer certificates.

The InterOp mode provides a backward compatibility to obsolete digital cinema servers which use the former InterOp standard. It is not recommended to use this option for current productions.

KDM Signature Setup

See chapter 5 KDM Signature.

Other Options

"Replicate Certificate Folder Structure" specifies if the output folder structure shall be the same as the input directory subfolder structure. This option only has effect when combined with the "Recursive" server certificate input folder option. E.g. an input folder "ServerCerts\" with a server certificate in a subfolder "ServerCerts\Cinema01\cert.cert" and an output directory "KDM\" will result in following output: "KDM\Cinema01\kdm.xml".

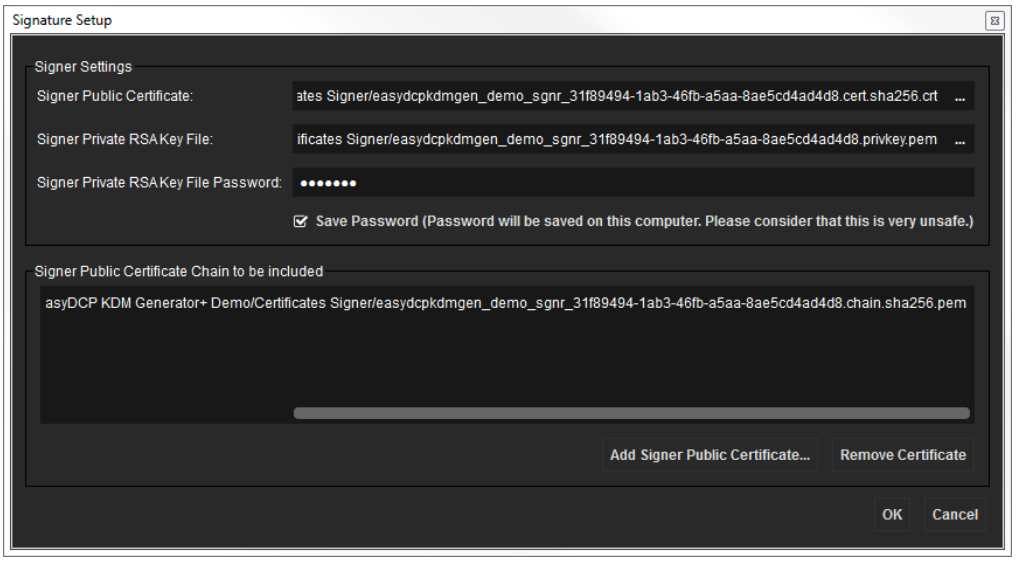
The "Show Signer Password in Output Window" option specifies, if the user password should be displayed with asterisks (*) or in plain-text in the output window. It is recommended to keep this option disabled.

5 KDM Signature

A valid KDM needs to be digitally signed by a signer certificate (leaf). This signer certificate is signed by another authority and that by another, and so forth until the last certificate in the certificate chain signs itself (root). Altering an existing KDM will lead to its invalidation. By inspecting the certificate chain, the KDM's recipients can decide if they trust the KDM or not.

In the demo version of easyDCP KDM Generator(+) an example signer certificate will be created at the first start up. Therefore users will be asked to specify a password. The signature setup dialog will be filled in with the auto-generated certificate automatically.

After licensing a commercial version of easyDCP KDM Generator(+) users may import the previously requested license and certificates by using the "Import License & Certificates" option in the help menu (see chapter 3.4). Doing so will automatically fill in the signature setup dialog with the imported signer certificate set. Of course, you may also use this dialog to set up another signature chain.


Signature Setup
Signer Settings
Signer Public Certificate:
ates Signer/easydcpkdmgen_demo_sgnr_31f89494-1ab3-46fb-a5aa-8ae5cd4ad4d8.cert.sha256.crt
Signer Private RSA Key File:
ificates Signer/easydcpkdmgen_demo_sgnr_31f89494-1ab3-46fb-a5aa-8ae5cd4ad4d8.privkey.pem
Signer Private RSA Key File Password:
Save Password (Password will be saved on this computer. Please consider that this is very unsafe.)
Signer Public Certificate Chain to be included
asyDCP KDM Generator+ Demo/Certificates Signer/easydcpkdmgen_demo_sgnr_31f89494-1ab3-46fb-a5aa-8ae5cd4ad4d8.chain.sha256.pem
Add Signer Public Certificate...
Remove Certificate
OK
Cancel

This dialog shows the currently used digital signature and certificate chain.

Signer Public Certificate

This field specifies the leaf certificate, which starts with "signer" and has a "crt" suffix. The signer certificate contains the signature's public key.

Signer Private RSA Key File

This field specifies a file that contains the signature's private key. The file is encrypted with a user password.

Signer Private RSA Key File Password

The password used to decrypt the signer's Signer Private RSA Key File. The default signature's user password is stored in a text file and read from there by default. When importing a custom chain, the user password may optionally also be stored in a text file. Note that this is potentially harmful as unauthorized access to the password may be possible and your digital signature may get compromised.

Signer Public Certificate Chain to be included

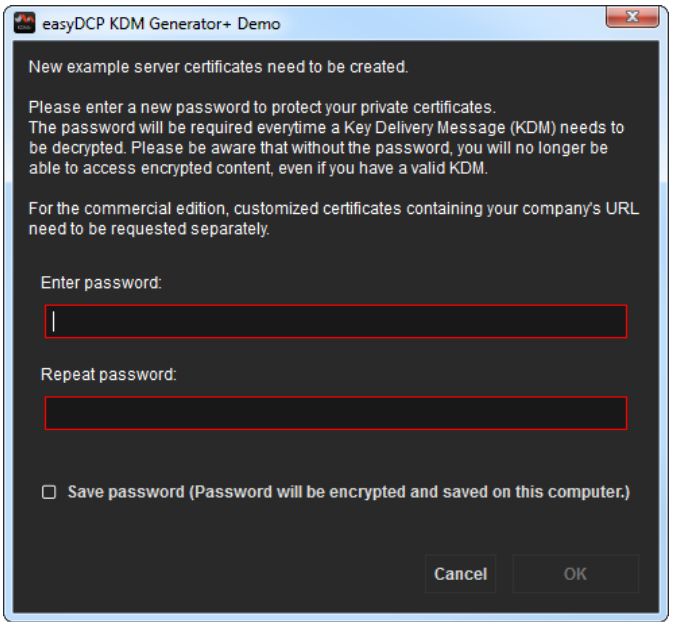
To complete the signer settings, the certificate chain's intermediate and root certificates need to be imported. To add a certificate, click the button "`Add Signer Public Certificate...`". To remove a certificate from the list, highlight it and click "`Remove Certificate`".

6 Distribution KDM

PLUSFeature

easyDCP KDM Generator+ can read Distribution KDMs (DKDM). A DKDM is technically identical to a regular KDM. The difference is that it targets another mastering station instead of a cinema server. A scenario would be if a post production house is contracted to create KDMs for a number of cinemas or a whole region or country. The supplier would provide a single DKDM issued to the post production house's easyDCP KDM Generator+ installation. This enables them to supply a new group of recipients with KDMs containing the same keys as the original DKDM. The procedure is identical to generating regular KDMs. The post production house does not even have to have a copy of the DCP itself.

Each installation manages its own private key and public key. The private key is known only to your easyDCP KDM Generator+ installation, whereas the public key is contained in a public server certificate and may be distributed to content providers. When content providers choose to encrypt a DCP, they need to somehow provide the decryption keys (there is one key for every encrypted track file) to the play out system or mastering station. To ensure that no one else is able to read these sensitive decryption keys, they are themselves encrypted in a way that only the targeted system is able to decrypt them. To do this, the content provider will need the recipient's public server certificate (export certificate with 'F7'). This encrypted message is called a Key Delivery Message (KDM). When the KDM does not target a digital cinema server, but rather another mastering station in the post-production or distribution chain, it is referred to as a Distribution KDM (DKDM). easyDCP KDM Generator+ does not keep loaded DKDMs in a repository.


easyDCP KDM Generator+ Demo
New example server certificates need to be created.
Please enter a new password to protect your private certificates.
The password will be required everytime a Key Delivery Message (KDM) needs to be decrypted. Please be aware that without the password, you will no longer be able to access encrypted content, even if you have a valid KDM.
For the commercial edition, customized certificates containing your company's URL need to be requested separately.
Enter password:
Repeat password:
Save password (Password will be encrypted and saved on this computer.)
Cancel
OK

When the easyDCP KDM Generator+ demo is first started, it will create a new random private key as well as a public server certificate. The certificate is digitally signed by four other certificates. These certificates are referred to as a certificate chain and this certificate chain, even though already included in the public server certificate, is additionally saved in a separate file. The certificate's critical private key is not only protected by a user password, but it is also asynchronously encrypted to ensure maximum security of encrypted DCP content. Likewise, if the user chooses to store their password for convenience, the saved data still needs to be asynchronously decrypted. The user password needs to have 8 to 12 letters and **cannot be changed after it was created**. The user will be prompted to specify a password when the application first launches.

The commercial edition, on the other hand, does not auto-generate certificates. Instead certificates are requested and imported with the "Request License & Certificates" and "Import License & Certificates" option in the help menu. These certificates are meant for commercial use as they state the licensee's URL and have a unique serial number that links the certificates to the license. Such certificates are tied to the machine's easyDCP system hash. When the license should need to be migrated to another machine, a new certificate set will have to be requested.

All mentioned files are stored in the user application data folder's certificates subfolder (see 6.1). Hence, the OS user management can be used to maintain multiple sets of certificates. In order to easily determine which files belong together, they are each identified by a unique ID. The ID of the set that is currently used by easyDCP KDM Generator+ is also listed in the "about" dialog (hit 'F6').

- easydcpkdmgen_<ID>.privkey.pem contains the encrypted private key
- easydcpkdmgen_<ID>.cert.sha256.crt is the public server certificate
- easydcpkdmgen_<ID>.chain.sha256.pem contains the certificate chain
- easydcpkdmgen_<_<ID>.privkey.passwd contains the encrypted user password

When easyDCP KDM Generator+ is uninstalled, none of these files will be removed. If the user password file (*.passwd) is manually deleted, the user will simply be prompted for the password again the next time a DKDM is loaded.

In the demo version, if any of the other three files are removed, all remaining files will be renamed (to <original filename>.bak) and a new private key along with new certificates will be created. The user will also be asked to specify a new password.

6.1 Application Data and Settings

easyDCP KDM Generator(+) automatically creates an application data folder. It contains a settings file as well a folder for its automatically generated certificates.

The settings file is used to store settings across program starts. It contains several user settings (e.g. default output folder, KDM conformity mode, signer certificates, etc) and will be refreshed each time easyDCP KDM Generator is closed. Most standard parameters can be set from within the graphical user interface.

On Windows, it is located in <User Application Data>/Fraunhofer IIS/easyDCP KDM Generator/ and <User Application Data>/Fraunhofer IIS/easyDCP KDM Generator+/

The user application data folder is often in "C:/Documents and Settings/<username>/Application Data/

On MacOS, it is located in \Users\<username>\Library\Application Support\Fraunhofer IIS\easyDCP KDM Generator\ or \Users\<username>\Library\Application Support\Fraunhofer IIS\easyDCP KDM Generator +\

7 Using the command line program

Apart of using the graphical user interface it is also possible to generate KDMs from the command line. This is handy in automatized environments or for embedding easyDCP KDM Generator in large workflows.

In Windows, the standard easyDCP KDM Generator.exe cannot directly print to the command line. Instead call easyDCP KDM Generator.com. On Mac, there is no such limitation.

To print all available arguments and flags, start easyDCP KDM Generator from the command line with the `-h` option.

7.1 Parameters

```
usage: easyDCP KDM Generator+ -d <DigestFile> -cpl <CplSelection> -i
<ServerCertificateFile|ServerCertificateFolder|FacilityListMessageFile> [-recursive] -l
<TrustedDeviceListCertificateFiles, TrustedDeviceListCertificateThumbprints> -o
<OutputFolder> [-replicate-structure] -tz <TimeZone> -s <ValidityStartTime> -e
<ValidityEndTime> -v <ValidityPeriodInDays> -k <SignerPrivateKeyFile> -p
<SignerPrivateKeyFilePassword> -a <AnnotationText> -c
<DisableForensicMarkingAudioChannelsAboveNumber [0-16]> [-t|-r] -w -n -h

usage: easyDCP KDM Generator+ -d <DistributionKDMFile> -m <ServerPrivateKeyFilePassword>
-cpl <CplSelection> -i <ServerCertificatesInputFolder|ServerCertificate> [-recursive] -l
<TrustedDeviceListCertificates, TrustedDeviceListThumbprints> -o <OutputFolder> [-
replicate-structure] -tz <TimeZone> -s <ValidityStartTime> -e <ValidityEndTime> -v
<ValidityPeriodInDays> -k <SignerPrivateKeyFile> -p <SignerPrivateKeyFilePassword> -a
<AnnotationText> -c <DisableForensicMarkingAudioChannelsAboveNumber [0-16]> [-t|-r] -w -
n -h -u

-d       DCP Digest File or Distribution KDM file (*.dcpdig, *.xml).
         The DCP Digest / Distribution KDM file holds the encryption
         keys for a specific DCP or composition thereof.
         WARNING: DIGEST FILES HOLD THE KEYS TO DECRYPT DCPS AND SHALL
         NOT BE DELIVERED TO A THEATER!
-cpl     Create KDM(s) only for a subset of composition containing the given
         string in thir title or uuid.
         If this pramaeter is not given KDM(s) will be generated
         for all composition.
-m       Password for the Server Certificate Private Key File,
         which is required to decrypt Distribution KDM(s).
-u       Save the password for decrypting your Distribution KDM(s).
         Please consider that this is very unsafe.
-i       Server Certificate input file of folder holding the
         Server Certificate(s) for which KDM(s) will be created.
-recursive
         Look for Server Certificates in subfolders also.
-l       Server Certificate input filenames or thumbprints of
         Trusted Device List (TDL) for which KDM(s) will be created.
         Filenames or thumbprints may be mixed and comma separated.
         If no input is given, the "assume trust" thumbprint
         "2jmj7l5rSw0yVb/vlWAYkK/YBwk=" will be added.
         NOTE: The parameters "-t" and "-l" are mutually exclusive.
-o       Path to output folder where the KDMs will be stored after creation.
-replicate-structure
         If the parameter -recursive is given, subfolder structure of the
         input Server Certificate directory will be replicated
         in the output directory.
```

```
         Otherwise this parameter has no effect.
-p       Password for the Signer Certificate Private Key File.
-tz      Target time zone for the KDM(s). The given date and times
         will be interpret as local date and times of this time zone.
         If no time zone is given local time zone of system will be used.
         To print a list of all valid time zones use -tz list .
         If times are given in UTC, this parameter is invalid.
-s       Start Time (as local or UTC time) for the validity period of the KDM.
         Following format expected: "YYYY-MM-DD[Thh:mm:ss[<+|->hh:mm]]"
         (e.g. 2014-05-06T08:44:47).
-e       End Time (as local or UTC time) for the validity period of the KDM.
         Following format expected: "YYYY-MM-DD[Thh:mm:ss[<+|->hh:mm]]"
         (e.g. 2014-05-08T08:44:47).
-v       Validity period in days from now on (e.g. 2)
-a       Annotation Text for the KDM. If no Annotation Text is given, the
         Content Title of the Composition Playlist (CPL) is used.
-t       Enforces "INTEROP" mode. NOTE: This setting is for backward
         compatibility only and is not recommended.
-r       Enforces "SMPTE" mode. NOTE: The parameters "-t" and
         "-r" are mutually exclusive. It is recommended to omit
         both switches in order to auto-detect the conformity based
         on the targeted server certificates.
-c       Disable Forensic Marking (FM) for audio channels above the given
         number. Values between 0 and 16 are permitted.
         If this parameter is omitted, FM will be enabled by default.
         If the input is a DKDM, FM flags will be carried over.
         The parameters "-t" and "-c" are mutually exclusive.
-naming-scheme
         Placeholders are:
         %1: CPL Content Title
         %2: Certificate File Name
         %3: KDM UUID
         %4: Date, user defined date and/or time format
         %5: Counter
-naming-scheme-date-format
         Date format for naming scheme.
-n       No pause after generation process (for automatic scripting purposes).
-w       Shows signer password in plain text instead of hidden text.
         (WARNING: This setting should only be used for debug purposes).
-h -?  -help
          Shows Help and Licensing Information.
```

7.2 Date and Time Specification

The command line allows more advanced date and time specifications for the *valid from* and *valid to* times. The parameters `-s` and `-e` are used for a concrete date and/or time. The values can be a date only, a date and time or a date and time with time zone offset. Date and time without time zone offset is interpreted as a local time. If no time zone is specified with the parameter `-tz` the current configured local time of the operating system will be used. Date and time with time zone offset will always be interpreted as UTC time. In this case the parameter `-tz` is invalid. To print a list of all available time zones use the parameter `-tz` with list, e.g. `-tz list`.

The parameter `-v` is used to specify a time-window in days beginning at the given start time. The resulting time-window of the generated KDM may deviate from the amount of specified days by plus or minus one hour. This is because easyDCP KDM Generator(+) takes daylight saving time (DST) into account. Therefore the local end time will always be the same as the local start time regardless if the start or end date is DST. E.g. if the start time is 13:30:00 local time, the end time will also be 13:30:00 local time.

8 Creating proper Digest Files

To generate your own digest file it is recommended to use an already existing digest file as a template. Open the file in an ordinary text editor. Afterwards it is possible to edit the specified fields with your own data and information.

If you have issues with an easyDCP Digest file, please contact the support. Detailed contact information can be found in chapter 10 (Contact).

9 Frequently Asked Questions (FAQs)

What does the KDM workflow look like with the easyDCP KDM Generator(+)?

easyDCP Creator+ generates a proprietary DCP digest file along with each encrypted DCP. This digest file contains all encrypted track files' keys. Whenever you want to generate KDMs, you can load this digest file into easyDCP KDM Generator(+). easyDCP KDM Generator (basic edition) is included in each purchase of easyDCP Creator+. All you need to do is collect your recipients' public server certificates and put them into a local folder. Use only the "cert.sha256" files. Usually, they have either a *.crt or *.pem suffix. In easyDCP KDM Generator, you merely need to load the digest file, point to the folder with the server certificates and specify the start and end dates of the KDMs' validity period. Upon clicking the "Generate KDM!" button, easyDCP KDM Generator(+) will create KDMs for all server certificates in a single job. Note, that a digest file may contain multiple compositions, but a KDM only ever contains keys for a single composition. Thus, easyDCP KDM Generator(+) will create <number of compositions in digest file> x <number of server certificates in folder> KDMs. Using the full version of easyDCP Player+, you can test the whole procedure by issuing a KDM to your easyDCP Player+'s public server certificate. By the way, this procedure is the same when you want to issue a Distribution KDM (DKDM) for your client's mastering station.

The demo version of easyDCP KDM Generator(+) is restricted in that it only generates KDMs with a maximum validity of 48 hours, starting from the time when the KDM is generated.

Where can I get the server certificates needed to create KDMs?

This is different in every country. We can’t send you the certificates. The best way is asking the cinema owner directly. They should either have the certificates of the projection system in their screening rooms themselves or tell you the model and serial number. If they give you the model and serial number, you need to contact the manufacturer and ask for access to their database. This is often a password protected ftp server. We can't give you the access details. For now, it is a good idea to maintain your own personal collection of certificates so you do not need to repeat this procedure for every job.

Why are there so many public certificates for a single cinema server?

Usually, on the cinema server manufacturers' ftp servers you can find both the public server certificate and the signature chain that was used to sign the certificate. If you decide to trust the certificate by examining the signature certificate chain, you only need the server certificate to create a KDM. It has either a *.pem or *.crt suffix. easyDCP KDM Generator(+) will accept either,

but do not use both. Furthermore, there will be pairs of certificate and chain that state "mpeg", "sha1" and "sha256". Like with DCPs, there are SMPTE and InterOp KDMs. Almost all modern servers prefer SMPTE KDMs. It is recommended to use the “Auto-detect” conformity option in order to infer the conformity from the targeted public server certificate (i.e. SMPTE for "sha256" certificates and InterOp for „sha1“ certificates).

Only if you know your recipient only accepts InterOp KDMs, use the "sha1" certificate.

How can I generate my own digital signature to sign my DCPs or KDMs?

Digital signatures are used to authenticate content. You can sign both DCPs and KDMs. For customers of easyDCP KDM Generator(+) we offer to generate signature chains for free.

We would only need to know your URL (without www), which is stated within the signature, e.g. "fraunhofer.de". Refer to chapter 5 for a guide on how to import the certificate chain.

My client wants me to send an encrypted DCP along with a Distribution KDM (DKDM). What is he talking about?

A Distribution KDM is technically identical to a regular KDM. The difference is that it targets another mastering station instead of a cinema server. A scenario would be if a post production house is contracted to add subtitles to a finished DCP. The supplier would send a copy of the encrypted DCP and issue a DKDM to the post production house's mastering station, enabling them to decrypt and alter the DCP. You can generate a DKDM with easyDCP KDM Generator(+). The procedure is identical to generating a regular KDM.

Can easyDCP KDM Generator issue new KDMs based on a DKDM?

Yes, but only easyDCP KDM Generator+ can. Please refer to chapter 6.

10 Contact

We very much appreciate any feedback or annotations about easyDCP KDM Generator(+). In order to enhance the software and to optimize it for your applications, we are looking forward to your cooperation.

If you have any problems or questions, please contact us at the following addresses:

Sales & Technical Support

easyDCP GmbH
Eiblwiesweg 2
82418 Murnau, Germany
info@easyDCP.com

Product Management

Fraunhofer Institute for Integrated Circuits IIS
Department Moving Picture Technologies
Heiko Sparenberg
91058 Erlangen, Germany
heiko.sparenberg@iis.fraunhofer.de